ONVEILIG GEDRAG OP INTERNET

De personen op de foto hebben geen relatie met de inhoud van het verhaal / foto: Liesbeth Dingemans

PRINT DIT ARTIKEL NAAR HOME

24 februari 2020

AUTEURS: SUSANNE VAN 'T HOFF-DE GOEDE , RICK VAN DER KLEIJ , STEVE VAN DE WEIJER , RUTGER LEUKFELDT

Veel burgers zijn de hele dag door online actief, maar hoe veilig gedragen zij zich op het internet? Bijvoorbeeld met het gebruik van wachtwoorden en online delen van persoonlijke gegevens. Dat valt tegen, blijkt uit onderzoek van de Haagse Hogeschool en het NSCR. Mensen gedragen zich onveiliger dan dat ze zelf zeggen dat ze doen.

Onze offline en online levens zijn zo met elkaar verweven dat burgers in Nederland de hele dag door allerlei online activiteiten uitvoeren. Online zijn levert echter ook gevaren op. Online criminaliteit is inmiddels veelvoorkomend en de impact ervan kan groot zijn voor slachtoffers. Een belangrijk deel van het slachtofferschap is terug te voeren op het gedrag van mensen. Gebruikers klikken immers op een hyperlink terwijl ze dat niet moeten doen. Of vullen gegevens in op een phishingwebsite waardoor criminelen die gegevens kunnen misbruiken. Om slachtofferschap terug te kunnen dringen is inzicht in het online gedrag van mensen dan ook van wezenlijk belang.

ONLINE GEDRAG

Het is tot op heden grotendeels onbekend hoe Nederlanders zich online gedragen en beschermen tegen online criminaliteit. Onder andere omdat hoe mensen zeggen zich online te gedragen, niet altijd hetzelfde is als hoe mensen zich daadwerkelijk online gedragen. Voor het empirisch onderbouwen van eventuele interventies op gedrag is dergelijke kennis echter onontbeerlijk.

Er bestaan grote verschillen tussen het zelfgerapporteerde gedrag en het objectieve gedrag

Daarom hebben de Haagse Hogeschool en het NSCR een onderzoek uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), om in kaart te brengen hoe veilig Nederlanders zich online zeggen te gedragen, hoe (on)veilig ze zich daadwerkelijk gedragen en welke verklaringen hiervoor zijn. Dit artikel bevat een

weergave van enkele opvallende bevindingen uit het onderzoeksrapport. Uiteraard is dit slechts een weergave van een beperkt aantal bevindingen. Voor wie meer wil lezen, of inzicht wil in verklarende variabelen verwijzen we naar het hele rapport.

ONDERZOEKSMETHODE

Om inzicht te krijgen in online gedrag hebben we gebruik gemaakt van een experimentele surveystudie. Daarin wordt de kracht van een vragenlijstonderzoek onder een representatieve groep burgers gecombineerd met de voordelen van experimenteel onderzoek, zoals het onder controle houden van verstorende variabelen. Voor deze studie maakten we gebruik van een steekproef van 2.426 volwassen Nederlanders.

In de survey werd online gedrag op 2 manieren gemeten: 1) door zelfrapportage, door enerzijds vragen en stellingen en anderzijds vignetten (korte situatieschetsen) voor te leggen aan de respondent; 2) daarnaast zijn respondenten tijdens het invullen van de vragenlijsten (fictieve) online risicosituaties tegengekomen, waarbij de onderzoekers bekeken hoe de respondenten met deze situaties omgaan. Dit vormde de metingen van het daadwerkelijke online gedrag van respondenten. Respondenten waren hiervan niet op de hoogte en dachten een vragenlijst in te vullen over wat voor online activiteiten ze uitvoeren (bijvoorbeeld online shoppen). Pas achteraf zijn de respondenten op de hoogte gebracht van de experimenten en het daadwerkelijke doel van het onderzoek.

GEDRAGSCLUSTERS

Het blijkt dat er grote verschillen bestaan tussen het zelfgerapporteerde gedrag en het objectieve gedrag zoals gemeten in onze experimenten. Uit de objectieve metingen blijkt steeds dat mensen zich onveiliger gedragen dan dat ze rapporteren te doen. Hieronder bespreken we beknopt de conclusies voor elk van de 4 gedragsclusters (gebruik van wachtwoorden, alertheid tijdens internetgebruik, online delen van persoonlijke gegevens en omgaan met bijlagen en hyperlinks in e-mails).

GEBRUIK VAN WACHTWOORDEN

Respondenten rapporteren zelf dat ze veilig omgaan met wachtwoorden. Ze geven aan geen wachtwoorden te delen en geen korte, makkelijke wachtwoorden te gebruiken. De sterkte van een wachtwoord is op verschillende manieren berekend, bijvoorbeeld de lengte van het wachtwoord en het gebruik van hoofdletters, kleine letters en leestekens.

zienlijk deel
in of haar
edatum

De objectieve metingen laten met betrekking tot het laatste een ander beeld zien: 89 procent van de respondenten heeft een zwak wachtwoord gebruikt. Zelfs als we alleen kijken naar de respondenten die aan het eind van de vragenlijst aangeven dat ze een wachtwoord hebben gekozen op dezelfde wijze als ze dat normaal zouden doen, dan blijkt dat ruim 83 procent een zwak wachtwoord gebruikt.

ALERTHEID TIJDENS INTERNETGEBRUIK

Bij het online alert zijn zien we eenzelfde beeld: respondenten geven middels zelfrapportage aan zich (zeer) veilig te gedragen (bijvoorbeeld niet downloaden uit illegale bron, geen gebruik maken van openbare wifi), terwijl uit de objectieve meting blijkt dat 40 procent van de respondenten onbekende software

downloadt als er een pop-up verschijnt tijdens een video die niet wil afspelen.

ONLINE DELEN VAN PERSOONLIJKE GEGEVENS

Bij het delen van persoonlijke gegevens geven de meeste respondenten aan zich bewust te zijn van de gevaren van het delen van persoonlijke gegevens (zoals een huisadres, e-mailadres of telefoonnummer) en connectieverzoeken via sociale media. Tijdens de objectieve meting blijken respondenten echter vaak bereid tot het opgeven van (zeer) persoonlijke gegevens. Respondenten werd gevraagd naar persoonlijke gegevens, waarbij het steeds mogelijk was om geen antwoord te geven. Een aanzienlijk deel geeft echter zijn of haar geboortedatum (37,5 procent), volledige naam (31 procent), e-mailadres (28,1 procent) en hun postcode (27,0 procent) en huisnummer (20,4 procent). Een klein maar toch substantieel deel van de respondenten (4,8 procent) is bovendien bereid tot het invullen van de laatste 3 cijfers van hun bankrekeningnummer.

OMGAAN MET BIJLAGEN EN HYPERLINKS IN E-MAILS

Respondenten rapporteren zich veilig te gedragen als het aankomt op het omgaan met bijlagen en hyperlinks in e-mails. Zo verwijderen respondenten heel vaak e-mails die zij niet vertrouwen en openen zij bijna nooit bijlagen in e-mails van onbekende afzenders.

ɡ gedrag blijkt
mate voor te

Uit vignetten die respondenten zijn voorgelegd – 3 e-mails waarvan 2 phishing-e-mails en 1 legitieme e-mail, waarbij ze moesten aangeven hoe ze zouden omgaan met de e-mails – blijkt echter dat 21 procent een onveilige handeling verricht: ze klikken op de hyperlink van een phishing-e-mail, of typen de URL over in de webbrowser.

ONVEILIG GEDRAG

Onveilig gedrag blijkt in hoge mate voor te komen. Zo gebruikt zo'n 80 procent een zwak wachtwoord, downloadt 40 procent onveilige software, en deelt ongeveer 30 procent van de respondenten persoonlijke gegevens, zoals hun volledige naam, geboortedatum en e-mailadres. Als respondenten phishing-e-mails krijgen voorgelegd dan blijkt dat ruim 20 procent een onveilige keuze maakt: ze klikken op de hyperlink of kopiëren de URL naar de webbrowser.

Het blijkt bovendien dat er grote verschillen bestaan tussen het zelfgerapporteerde gedrag en het daadwerkelijke gedrag. Uit de objectieve metingen blijkt steeds dat mensen zich onveiliger gedragen dan dat ze rapporteren te doen. We benadrukken daarom het belang van het doen van objectieve metingen van online gedrag.

EEN DOORKIJKJE: INTERVENTIES

Het doel van dit onderzoek was niet alleen om in kaart te brengen hoe Nederlanders zich online gedragen en dit te verklaren, maar ook om een eerste aanzet te geven om interventies te ontwikkelen om Nederlanders zich online veiliger te laten gedragen. De resultaten van dit onderzoek zijn dan ook bediscussieerd met experts om veelbelovende richtingen voor interventies te identificeren.

ɐn panacee voor
ɔrderen van
ıline gedrag

Samenvattend blijkt dat er geen panacee is voor het bevorderen van veilig online gedrag. Experts zien veel waarde in interventies die zich richten op

aanpassingen van de techniek die mensen gebruiken voor online activiteiten, dusdanig dat de mogelijkheid voor onveilig gedrag wordt verkleind en de mogelijkheid voor veilig gedrag wordt vergroot, ook wel security-by-design genoemd. Het stimuleren van fabrikanten van technologie via beleidsmaatregelen tot het maken van aanpassingen die het voor gebruikers makkelijker maakt om zich veilig te gedragingen, kan hieraan bijdragen. Daarnaast zou toekomstig onderzoek zich ook kunnen richten op het ontwikkelen en evalueren van een specifieke set van interventies voor het beïnvloeden van de door ons gevonden onveilige gedragingen.<<

Susanne van 't Hoff-de Goede is werkzaam bij de Haagse Hogeschool, Rick van der Kleij bij de Haagse Hogeschool en TNO, Steve van de Weijer bij het NSCR en Rutger Leukfeldt bij het NSCR en de Haagse Hogeschool. Rutger Leukfeldt is beschikbaar voor vragen en discussies via e-mail: RLeukfeldt(at)nscr.nl.

Dit artikel is gebaseerd op het onderzoek Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders. *In dit artikel is lang niet al het (zelf)gerapporteerde online gedrag van respondenten besproken en zijn ook de verklaringen niet aan bod gekomen. Daar is eenvoudigweg niet voldoende ruimte voor. Wie een compleet beeld wil verwijzen we naar het onderzoeksrapport*.